REMARKS

In the Office Action mailed on July 3, 2003, the Examiner objected to claim 17 and rejected claim 51 under 35 U.S.C. § 112, ¶ 2. The Examiner further: (1) rejected claims 1-9 and 12-51 under 35 U.S.C. § 102(e) as being anticipated by Johnson et al. (U.S. Pat. No. 5,870,740) ("Johnson"); and (2) rejected claims 10, 11, 21, 22, 32, 33, 43, 44, 49, and 50 under U.S.C. § 103(a) as being unpatentable over Johnson in view of Adams et al. (U.S. Pat. No. 6,031,911) ("Adams").

By this Amendment, Applicants cancel claims 17 and 51, without prejudice or disclaimer of the subject matter thereof, and respectfully traverse the rejection of pending claims 1-16 and 18-50 for the reasons given below.

1. Rejection of claims 1-9 and 12-51

Applicants respectfully traverse the rejection of claims 1-9 and 12-16, 18-50 under 35 U.S.C. § 102(e) as being anticipated by Johnson. As noted above, Applicants have canceled claims 17 and 51 and thus this rejection as to those claims is moot.

Claim 1 is patentable at least because Johnson does not teach each and every limitation of claim 1. Specifically, Johnson does not teach an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output. Instead, Johnson is directed to solving a particular problem with public key encryption systems that use a public elliptic curve key (col. 1, ll. 42-62). Specifically, in discussing the problem with existing elliptic curve encryption systems, Johnson notes that a user A may use a public elliptic curve key to encrypt a symmetric key (e.g., a DES key) for distribution to a user B. Johnson further notes that doing so, however, creates a problem because the symmetric key (e.g., the DES key) is typically

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

contained in a 512-bit block, whereas the elliptic encryption block is typically only 160 bits long (col. 1, l.63-col. 2, l. 3). Johnson notes that, while dividing the 512-bit block into multiple smaller blocks will work, it is computationally inefficient, and instead Johnson proposes a method of key encryption said to be usable with the elliptic curve keys. The method of key encryption taught by Johnson includes generating a masked plaintext block and then encrypting only a portion of that masked plaintext block (col. 2, ll. 16-37). A ciphertext is then generated from the encrypted portion of the masked plaintext block and the remaining portion of the masked plaintext block. *Id.* The ciphertext, including both the encrypted and unencrypted portions, is then transmitted to a recipient, who reverses the process to recover the original plaintext block. *Id.* Fig. 6 of Johnson shows the process for recovering the original plaintext block, including unmasking procedure 630. Thus, Johnson teaches a system in which masking of the plaintext occurs at the transmission side (encrypting side) and the unmasking occurs at the receiving side (decrypting side), but not both at the same side.

In contrast, claim 1 recites an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output. Thus, because Johnson does not teach each and every limitation of claim 1, it does not anticipate claim 1. Accordingly, Applicants respectfully deem claim 1 allowable over Johnson.

Claims 4, 8, and 9 depend from claim 1 and thus are patentable for at least the reasons given above with respect to claim 1.

Claim 2 is also patentable over Johnson because Johnson does not teach an encryption apparatus including means for removing an influence of the mask a from

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

intermediate bit data masked by a masking means for at least the same reasons as given above with respect to claim 1. Thus, Applicants respectfully deem claim 2 allowable over Johnson as well.

Claim 5 depends from claim 2 and thus is patentable for at least the reasons given above with respect to claim 2.

Claim 3 is also patentable over Johnson because Johnson does not teach an encryption apparatus including means for removing an influence of the mask a from an output from a data translation means which is masked by a masking means for at least the same reasons as given above with respect to claim 1. Thus, Applicants respectfully deem claim 3 allowable over Johnson as well.

Claims 6 and 7 depend from claim 3 and thus are patentable for at least the reasons given above with respect to claim 3.

Claim 12 is patentable over Johnson because Johnson does not teach a decryption apparatus including means for masking bits dependent on a ciphertext within the apparatus with mask patterns selected by a selection means. This is because, as discussed above with respect to claim 1, Johnson is directed to solving a particular problem with public key encryption systems that use a public elliptic curve key (col. 1, ll. 42-62). The method of key encryption taught by Johnson includes generating a masked plaintext block and then encrypting only a portion of that masked plaintext block (col. 2, ll. 16-37). A ciphertext is then generated from the encrypted portion of the masked plaintext block and the remaining portion of the masked plaintext block. *Id.* The ciphertext, including both the encrypted and unencrypted portions, is then transmitted to a recipient, who reverses the process to recover the original plaintext block. *Id.* Fig. 6

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

of Johnson shows the process for recovering the original plaintext block, including unmasking procedure 630. Thus, Johnson teaches a system in which masking of the plaintext occurs at the transmission side (encrypting side) and the unmasking occurs at the receiving side (decrypting side), but not both at the same side. Accordingly, because Johnson does not teach a decryption apparatus including means for masking bits dependent on a ciphertext within the apparatus with mask patterns selected by a selection means, Applicants respectfully deem claim 12 allowable over Johnson as well.

Claims 15, 19, 21, and 22 depend from claim 12 and thus are patentable for at least the reasons given above with respect to claim 12.

Claim 13 is also patentable over Johnson because Johnson does not teach a decryption apparatus including means for masking intermediate bit data within the apparatus with mask patterns selected by a selection means for at least the same reasons as given above with respect to claim 12. Thus, Applicants respectfully deem claim 13 allowable over Johnson as well.

Claims 16 and 20 depend from claim 13 and thus are patentable for at least the reasons given above with respect to claim 13.

Claim 14 is also patentable over Johnson because Johnson does not teach a decryption apparatus including means for masking an input to a data translation means with mask patterns selected a selection means for at least the same reasons as given above with respect to claim 12. Thus, Applicants respectfully deem claim 14 allowable over Johnson as well.

Claim 18 depends from claim 14 and thus is patentable for at least the reasons given above with respect to claim 14.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

Claim 23 is also patentable over Johnson because Johnson does not teach an encryption method including removing an influence of a mask a from a ciphertext before the ciphertext is output for at least the same reasons as given above with respect to claim 1. Thus, Applicants respectfully deem claim 23 allowable over Johnson as well.

Claims 26, 30, and 31-33 depend from claim 23 and thus are patentable for at least the reasons given above with respect to claim 23.

Claim 24 is also patentable over Johnson because Johnson does not teach an encryption method including removing an influence of a mask a from masked intermediate bit data for at least the same reasons as given above with respect to claim 1. Thus, Applicants respectfully deem claim 24 allowable over Johnson as well.

Claim 27 depends from claim 24 and thus is patentable for at least the reasons given above with respect to claim 24.

Claim 25 is also patentable over Johnson because Johnson does not teach an encryption method including removing an influence of the mask a from a masked output from a data translation step for at least the same reasons as given above with respect to claim 1. Thus, Applicants respectfully deem claim 25 allowable over Johnson as well.

Claims 28 and 29 depend from claim 25 and thus are patentable for at least the reasons given above with respect to claim 25.

Claim 34 is also patentable over Johnson because Johnson does not teach a decryption method including masking bits dependent on a ciphertext within the method with selected mask patterns for at least the same reasons as given above with respect to claim 12. Thus, Applicants respectfully deem claim 34 allowable over Johnson as well.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

Claims 37 and 41-44 depend from claim 34 and thus are patentable for at least the reasons given above with respect to claim 34.

Claim 35 is also patentable over Johnson because Johnson does not teach a decryption method including masking intermediate bit data within the method with selected mask patterns for at least the same reasons as given above with respect to claim 12. Thus, Applicants respectfully deem claim 35 allowable over Johnson as well.

Claim 38 depends from claim 35 and thus is patentable for at least the reasons given above with respect to claim 35.

Claim 36 is also patentable over Johnson because Johnson does not teach a decryption method including masking an input to a data translation step with selected mask patterns for at least the same reasons as given above with respect to claim 12. Thus, Applicants respectfully deem claim 36 allowable over Johnson as well.

Claims 39 and 40 depend from claim 36 and thus are patentable for at least the reasons given above with respect to claim 36.

Claim 45 is also patentable over Johnson because Johnson does not teach a computer-readable program code means for converting a plaintext block into a ciphertext block including computer-readable code means for causing a computer to remove an influence of the mask a from a ciphertext before the ciphertext is output for at least the same reasons as given above with respect to claim 1. Thus, Applicants respectfully deem claim 45 allowable over Johnson as well.

Claim 46 is also patentable over Johnson because Johnson does not teach an encryption apparatus including for removing an influence of the mask a from an output from a data translation means for at least the same reasons as given above with

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

respect to claim 1. Thus, Applicants respectfully deem claim 46 allowable over Johnson as well.

Claims 47-50 depend from claim 46 and thus are patentable for at least the reasons given above with respect to claim 46.

2. Rejection of claims 10, 11, 21, 22, 32, 33, 43, 44, 49, and 50

Applicants respectfully traverse the rejection of claims 10, 11, 21, 22, 32, 33, 43, 44, 49, and 50 under U.S.C. § 103(a) as being unpatentable over Johnson in view of Adams. Applicants respectfully submit that Johnson, even when combined with Adams, does not teach or suggest the claimed subject matter. This is because, as noted above, claims 10 and 11 depend from claim 1, and Johnson does not teach or suggest an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output, as recited in claim 1. Adams does not cure the deficiency of teachings of Johnson. Adams is directed to constructing large substitution boxes for use in improving the security of symmetric block ciphers (col. 1, ll. 10-14). Adams, however, does not teach or suggest an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output, as recited in claim 1. Thus, claims 10 and 11, which depend from claim 1, are patentable over Johnson and Adams, taken alone or in combination.

Claims 21 and 22 depend from claim 12 and are patentable even when Johnson is combined with Adams, because these two references do not teach or suggest a decryption apparatus including means for masking bits dependent on a ciphertext within the apparatus with mask patterns selected by a selection means for at least the reasons

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

discussed above with respect to claims 1 and 10-12. Thus, claims 21 and 22, which depend from claim 12, are patentable over Johnson and Adams, taken alone or in combination.

Claims 32 and 33 depend from claim 23 and are patentable even when Johnson is combined with Adams, because these two references do not teach or suggest an encryption method including removing an influence of a mask a from a ciphertext before the ciphertext is output for at least the reasons discussed above with respect to claims 1, 10, 11, and 23. Thus, Applicants respectfully deem claims 32 and 33 patentable over Johnson and Adams, taken alone or in combination.

Claims 43 and 44 depend from claim 34 and are patentable even when Johnson is combined with Adams, because these two references do not teach or suggest a decryption method including masking bits dependent on a ciphertext within the method with selected mask patterns for at least the same reasons as given above with respect to claims 10-12 and 34. Thus, Applicants respectfully deem claims 43 and 44 patentable over Johnson and Adams, taken alone or in combination.

Claims 49 and 50 depend from claim 46 and are patentable even when Johnson is combined with Adams, because these two references do not teach or suggest an encryption apparatus including for removing an influence of the mask a from an output from a data translation means for at least the same reasons as given above with respect to claims 1, 10, 11, and 46. Thus, Applicants respectfully deem claims 49 and 50 patentable over Johnson and Adams, taken alone or in combination.

Finally, the Office Action contains a number of statements reflecting characterizations of the claims and/or the related art. Regardless of whether any such

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

statements are addressed by Applicants' remarks above, Applicants decline to automatically subscribe to any of these statements or characterizations made by the Examiner in the Office Action.

In view of the foregoing amendments and remarks, Applicants respectfully request reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: October 2, 2003

By: _____
Ranjeev K. Singh
Reg. No. 47,093

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com